paloalto TECHDOCS

Prisma Access（中国地区）

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

February 8, 2024

Table of Contents

中国地区的 Prisma Access

在何处可以使用？	需要提供什么？

• Prisma Access (Managed by Panorama)
• Prisma Access (Managed by Strata Cloud Manager)
	• Prisma Access China 许可证
	• 仅限 Prisma Access (Managed by Panorama) 部署：
	  • Panorama 的最低版本为 10.2.4
	  • 云服务插件的最低版本为 4.1.0-h20
	• Prisma Access显式代理
	  • Prisma Access数据平面 10.2.10
	  • Global Protect 版本 6.2.3
	  • Panorama 插件版本 5.2.0

向混合劳动力的快速过渡，员工现在可以在公司办公室、分支机构、家庭办公室或路上流畅地工作（包括在中国地区的组织），这加速了业务开展方式和地点的变化。您可以使用 Prisma Access 保护位于中国的移动用户、分支机构以及总部和数据中心。如果您的组织当前使用显式代理和 PAC 文件，则可以从传统或基于云代理的安全 Web 网关 (SWG) 解决方案无缝过渡到 Prisma Access。这对于保护移动用户的互联网接入特别有利。此外，Prisma Access 显式代理功能非常适合出于合规性原因而需要使用代理的组织，以及为了保护部署在非默认路由网络中的端点而需要使用代理的组织。

中国地区的 Prisma Access 实例在中国托管，并且在遵守所有法规和要求的同时管理组织的网络安全基础设施。更重要的是，Prisma Access China 实现了一致的最终用户体验，将一致的可见性和控制能力扩展到中国大陆境内的位置。

在中国大陆上线 Prisma Access 地点时要使用的程序与在全球其他地点上线 Prisma Access 部署时要使用的程序相同。但是，请确保您了解以下差异：

- 部署类型（新的或现有的） — 您只能在新的 Prisma Access 环境中部署 Prisma Access China。不支持从现有 Prisma Access 部署进行升级或迁移。
- 部署类型（**Panorama** 或云托管**Prisma Access**） — 云托管和 Panorama 托管Prisma Access部署都支持 Prisma Access China。
- 所需的 **SKU** — 当您为在中国大陆的部署购买 Prisma Access 时，需要特定于 Prisma Access China 的 SKU。与您的 Palo Alto Networks 授权代表或合作伙伴合作，确保为您的 Prisma Access China 部署购买正确的 SKU。
- 支持的 **Panorama** 版本（仅限 Prisma Access (Managed by Panorama) 部署）— 如果您决定使用 Prisma Access (Managed by Panorama)，Prisma Access China 需要在中国进行特别构建；在开始安装之前，必须从以下中国大陆地区可用的映像之一部署硬件或虚拟（AWS、KVM 或 ESXi）Panorama 设备。
  - Panorama-AWS-10.2.3 (AWS)

- Panorama-KVM-10.2.3-h4.qcow2 (KVM)
- 以下 ESXi 映像中的一个或多个：
  - 如果您的部署不使用云身份引擎来进行身份验证，请下载并安装此映像：Panorama-ESX-10.2.3-h4.ova
  - 如果您的部署使用云身份引擎进行身份验证，请下载并安装 Panorama-ESX-10.2.3-h4.ova 映像，然后在 ova 映像上下载并安装此映像：Panorama_pc-10.2.4-ch139

    此外，如果您的部署使用云身份引擎，请联系您的 Palo Alto Networks 团队，他们将建立案例并复制正确的证书颁发机构 (CA) 证书，以便在中国与云身份引擎一起使用。

仅将新的 Panorama 设备用于 Prisma Access China。仅使用此设备管理 Prisma Access China，请勿将其用于管理内部防火墙。

- 所需的 **Panorama** 物理位置（仅限 Panorama 托管的部署）— 您用于管理 Prisma Access China 的 Panorama 必须安装在中国大陆地区的地点。如果是硬件设备，则必须位于中国大陆地区；如果是 Panorama 虚拟设备，则实例化设备的云位置必须位于中国地区。
- 支持的地点 — Prisma Access China 支持中国大陆地区的以下地点。
- 支持的 **Strata Logging Service** 区域 — Prisma Access China 仅支持 Strata Logging Service China 区域，在产品激活期间，会自动为您填充该区域。

  如果您想启用从位于中国的 *Strata Logging Service* 到外部日志服务器的日志转发，则需要更改中国的 *Prisma Access* 基础架构。请联系您的 *Palo Alto Networks* 团队，以便开始转发日志。请注意，如果配置日志转发配置文件来将日志发送到位于中国以外的服务器，可能会导致个人身份信息离开中国。
- 所需的 **GlobalProtect** 版本 — Prisma Access China 支持标准 Prisma Access 部署中支持的所有 GlobalProtect 版本。
- 功能支持 — Prisma Access 支持位于中国的移动用户 — 显式代理部署。您可以使用以下方法之一进行连接：
  - 代理模式下的 GlobalProtect
  - 隧道和代理模式下的 GlobalProtect
  - PAC 文件与 Kerberos
  - 代理模式与远程网络

  位于中国的 Prisma Access 显式代理仅支持互联网和 SaaS 应用程序。

  不支持使用 SAML 身份验证的 PAC 文件、IP 地址优化、远程网络上具有代理模式的私有 IP 地址可见性。

  如果您使用 *Strata Cloud Manager* 来管理显式代理部署，请联系您的 *Palo Alto Networks* 客户代表，以便在中国地区启用显式代理。
- 移动用户 **IP** 地址支持 — 在 Prisma Access 部署中配置移动用户 IP 地址池时，请仅使用全球池。选择区域或地点组地址可能在提交时出错。
- 所需的云服务插件版本 — 4.1.0-h20

  如果您运行的插件版本早于 4.1.0-h20（例如 3.2.1-h18），则应将插件升级到所需的最低版本。

- 功能支持 — 除以下附加组件和功能外，所有功能和附加组件均受 Prisma Access China 支持：
  - 基本 **Prisma Access** 功能 — 不支持以下 Prisma Access 功能：
    - 对远程网络位置的安全入站访问
    - Autonomous DEM (ADEM) 附加组件

    有关不受支持的功能的详细列表，请联系您的 Palo Alto Networks 代表。
  - 要通过跨境线路（例如，MPLS 线路）访问位于中国境外的外部 SaaS 应用或其他外部互联网资源，您可以使用流量转向功能，在将移动用户或远程网络流量发送到互联网之前，将其重定向到服务连接。
  - **GlobalProtect** 门户名称更改 — Prisma Access China 的 GlobalProtect 门户名称是 *<portal-name>*`.prismaaccess.cn`。
  - 其他 **Prisma Access** 组件和附加组件的兼容性 — 支持的附加组件取决于许可类型以及客户的隐私配置文件和治理。Prisma Access China 提供了两种许可证：1 级许可证提供了一种解决方案，可限制从中国大陆地区导出个人身份信息 (PII) 的数量，2 级许可证允许更多不限制将数据导出到中国境外的附加组件和功能。

  下表显示了对其他 Prisma Access 组件和附加组件的支持；复选标记 (√) 表示支持，破折号 (—) 表示不支持：

组件或附加组件	**1** 级许可证支持（仅限 **Panorama**）	**2** 级许可证支持
通过服务连接访问私有应用	√ 对于企业许可证，许可证提供五个服务连接。对于商业高级版和企业版许可证，可以附加组件的形式提供附加服务连接。	√ 对于企业版许可证，许可证提供五个服务连接。对于商业高级版和企业许可证，可以附加组件的形式提供附加服务连接。
标准威胁防护	√	√
高级威胁防护	—	√
标准 URL 过滤	√	√
高级 URL 过滤	—	√
DNS 安全	√	√
Advanced WildFire	—	√
新一代 Cloud Access Security Broker (CASB-X)	—	√（作为附加组件提供）
Enterprise DLP	—	√（作为附加组件提供）

组件或附加组件	**1** 级许可证支持（仅限 **Panorama**）	**2** 级许可证支持
SaaS Inline	—	√（作为附加组件提供）
IoT Security	—	√（作为附加组件提供）

在中国大陆地区上线移动用户和分支机构

在何处可以使用？	需要提供什么？

• Prisma Access（Panorama 托管）
• Prisma Access（云托管）
	• Prisma Access China 许可证
	• 仅 Panorama 托管的部署：
	  • 最低 Panorama 版本为 10.2.3-h410.2.4
	  • 最低云服务插件版本为 3.2.1-h184.1.0-h20

向混合劳动力的快速过渡，员工现在可以在公司办公室、分支机构、家庭办公室或路上流畅地工作（包括在中国地区的组织），这加速了业务开展方式和地点的变化。您可以使用 Prisma Access 来保护中国地区的移动用户、分支机构以及总部和数据中心位置，并允许加密流量，从而与中国境外的应用程序和数据通信，同时确保在中国大陆内外的合法性和合规性。

中国地区的 Prisma Access 实例在中国托管，并且在遵守所有法规和要求的同时管理组织的网络安全基础设施。更重要的是，Prisma Access China 实现了一致的最终用户体验，将一致的可见性和控制能力扩展到中国大陆境内的位置。

在中国大陆地区上线 Prisma Access 位置所需遵循的程序与上线 Prisma Access 服务连接、远程网络连接和移动用户（全球其他位置的 GlobalProtect 部署）所需遵循的程序相同。但是，请确保您了解以下差异：

- 部署类型（新的或现有的）— 只能在新的 Prisma Access 环境中部署 Prisma Access China。不支持从现有 Prisma Access 部署进行升级或迁移。
- 部署类型（**Panorama** 或云托管**Prisma Access**）— 仅 Panorama 管理的 Prisma Access 部署支持 Prisma Access China；不支持云托管的 Prisma Access 部署。
- 所需的 **SKU** — 为在中国大陆的部署购买 Prisma Access 时，需要特定于 Prisma Access China 的 SKU。与 Palo Alto Networks 授权代表或合作伙伴合作，确保为您的 Prisma Access China 部署购买正确的 SKU。
- 支持的 **Panorama** 版本 — Prisma Access China 需要在中国进行特别构建；在开始安装之前，必须从以下中国大陆地区可用的映像之一部署硬件或虚拟（AWS、KVM, 或 ESXi）Panorama 设备。
  - Panorama-KVM-10.2.3-h4.qcow2
  - Panorama-ESX-10.2.3-h4.ova
  - Panorama-AWS-10.2.3

  对于 Prisma Access China，您必须使用新的 Panorama 设备。该 Panorama 只能用于管理 Prisma Access China，不能用于管理本地防火墙。
- 所需的 **Panorama** 物理位置 — 用于管理 Prisma Access China 的 Panorama 必须安装在中国大陆地区。如果是硬件设备，则必须位于中国大陆地区；如果是 Panorama 虚拟设备，则实例化设备的云位置必须位于中国地区。

- 支持的地点 — Prisma Access China 支持中国大陆地区的以下地点：
  - 华北 — 北京（使用华北计算位置）
  - 西北 — 宁夏（使用西北计算位置）
- 支持的 **Strata Logging Service** 地区 — Prisma Access China 仅支持 Strata Logging Service China 区域，系统会自动为您填充。
- 所需的 **GlobalProtect** 版本 — Prisma Access China 支持标准 Prisma Access 部署中支持的所有 GlobalProtect 版本。
- 所需的最低云服务插件版本 — 3.2.1-h18
- 功能支持 — Prisma Access 支持在中国地区的移动用户 — 显式代理部署。但是，以下功能不受支持：
  - Explicit 代理的 Cloud NAT 支持
  - 专用应用访问权限
  - SAML 或 CIE 身份验证
  - SASE-IA
  - Prisma Access 事件和警报
  - Prisma Access 浏览器
  - 远程网络和具有私有 IP 可见性功能的显式代理

  请联系您的 *Palo Alto Networks* 客户代表，以便在中国地区启用 *Strata Cloud Manager* 上的显式代理。
- 功能支持 — 除以下附加组件和功能外，Prisma Access China 支持所有其他功能和附加组件：
  - 基础 **Prisma Access** 功能 — 不支持以下 Prisma Access 功能：
    - 对远程网络位置的安全入站访问
    - Autonomous DEM (ADEM) 附加组件
    - 云管理

    有关不支持的功能的详细列表，请联系您的 Palo Alto Networks 代表。
  - 要通过跨境线路（例如 MPLS 线路）访问中国境外的外部 SaaS 应用程序或其他外部互联网资源，您可以使用流量定向来将移动用户或远程网络流量重定向到服务连接，然后发送到互联网。
  - **GlobalProtect** 门户名称更改 — Prisma Access China 的 GlobalProtect 门户名称是 *<portal-name>*`.prismaaccess.cn`。
  - 其他 **Prisma Access** 组件和附加组件的兼容性 — 支持的附加组件取决于许可类型以及客户的隐私配置文件和治理。Prisma Access China 提供了两种许可证：1 级许可证提供了一种解决方案，可限制从中国大陆地区导出个人身份信息 (PII) 的数量，2 级许可证允许更多不限制将

数据导出到中国境外的附加组件和功能。下表显示了对其他 Prisma Access 组件和附加组件的支持；复选标记 (√) 表示支持，波折号 (—) 表示不支持：

组件或附加组件	1 级许可证支持	2 级许可证支持
通过服务连接访问专用应用	√ 对于 Enterprise 许可证，随许可证提供了五个服务连接。对于 Business Premium 和 Enterprise 许可证，附加服务连接可作为附加组件使用。	√ 对于 Enterprise 许可证，随许可证提供了五个服务连接。对于 Business Premium 和 Enterprise 许可证，附加服务连接可作为附加组件使用。
标准威胁防护	√	√
高级威胁防护	—	√
标准 URL 过滤	√	√
高级 URL 筛选	—	√
DNS 安全	√	√
Advanced WildFire	√ 您可以选择和取消选择 Advanced WildFire 会话信息设置中的字段，以禁止发送 PII。	√
新一代云访问安全代理 (CASB-X)	—	√（作为附加组件提供）
企业 DLP	—	√（作为附加组件提供）
SaaS 内联	—	√（作为附加组件提供）
IoT Security	—	√（作为附加组件提供）

配置 Prisma Access China 部署

在何处可以使用？	需要提供什么？

• Prisma Access (Managed by Strata Cloud Manager) 托管）
• Prisma Access (Managed by Panorama)
	• Prisma Access China 许可证
	• 仅限 Prisma Access (Managed by Panorama)：
	  • 最低 Panorama 版本为 10.2.3-h410.2.4
	  • 最低云服务插件版本为 3.2.1-h184.1.0-h20

查看安装 Prisma Access China 的安装要求后，请执行以下步骤以完成设置。

STEP 1 | （可选）创建专用于部署 Prisma Access China 的客户支持门户 (CSP) 帐户。

虽然不要求为 Prisma Access China 创建专用的 CSP 帐户，但您可能会发现创建一个专用帐户很有用，因为 Prisma Access 设置和激活是特定于 Prisma Access China 的。

STEP 2 | （仅限 Prisma Access (Managed by Panorama) 部署）安装 Panorama，它将用于管理位于中国地区的 Prisma Access（如果未安装）。

查看支持的 Panorama 版本，获取映像链接和安装 Panorama 的说明。

STEP 3 | 激活并安装 Prisma Access China 部署。

STEP 4 | 激活并安装 Prisma Access China 部署（云托管或Panorama 托管）。

STEP 5 | （可选，仅限 Prisma Access (Managed by Panorama) 部署）如果您需要安装 Panorama 设备证书（**Panorama** > **Setup**（设置） > **Device Certificate**（设备证书）），请在下载之前通过管理 Prisma Access 的 Panorama 打开 CLI 会话并输入以下 CLI 命令：

```
request certificate secure-bridge enable
```

在下载证书之前输入此命令可确保获得在中国签名的证书。

STEP 6 | 将以下 URL、IP 地址和端口添加到要与 Prisma Access 配合使用的任何安全设备上的允许列表中。

此外，对于 Prisma Access (Managed by Panorama) 部署，如果 Panorama 设备使用代理服务器（**Panorama** > **Setup**（设置） > **Service**（服务） > **Proxy Server**（代理服务器）），或者如

果您对 Prisma Access 使用 SSL 转发代理，请确保将以下 URL、IP 地址和端口添加到代理或代理服务器上的允许列表中。

- api.prismaaccess.cn（对于 Prisma Access）
- api.sb.prismaaccess.com（对于 Prisma Access）
- api-trusted.sb.prismaaccess.com（对于 Prisma Access）
- *.proxy.prismaaccess.cn（用于 Prisma Access 显式代理）
- 中国地区 Strata Logging 服务所需的 FQDN、端口和 IP 地址
- Panorama 使用的端口。

STEP 7 | （仅限 Prisma Access (Managed by Panorama) 部署）选择 **Device**（设备） > **Setup**（设置） > **WildFire**并输入 **`cn.wildfire.paloaltonetworks.com`**。

您必须将 WildFire China Cloud 与 Prisma Access China 一起使用。

STEP 8 | 配置 Prisma Access 服务基础设施。

STEP 9 | 如果您有“移动用户 — GlobalProtect”部署，请配置您的部署。

Palo Alto Networks 建议第一步使用本地身份验证，以便验证是否已设置服务以及您的用户是否可以访问互联网。稍后可以切换为使用公司身份验证方法。

STEP 10 | 启用服务基础架构和允许 Prisma Access 元素之间进行通信的服务连接。

STEP 11 | 计划并创建一个服务连接来保护对私有应用的访问。

STEP 12 | 计划、创建和配置远程网络连接来保护对分支机构站点的访问。

STEP 13 | 检索Prisma Access公共和私有 IP 地址并将其添加到组织的网络允许列表中。

添加这些地址以限制对企业网络和应用程序的入站访问。

（仅限 *Prisma Access (Managed by Panorama)* 部署）如果您有“移动用户 — *GlobalProtect*”部署，则可以使用 Prisma Access UI（而不是此 *API*）来管理公共 *IP* 地址分配，并在 *Prisma Access* 释放这些 *IP* 地址之前确认已将其添加到允许列表中。这样，*Prisma Access* 就只会配置允许列表中的 *IP* 地址。

STEP 14 | （可选）将身份验证方法从本地身份验证更改为组织的身份验证方法，并为移动用户设置身份验证。

